IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

SHENIQUA ROWE, Plaintiff, vs. **PAPA JOHN'S INTERNATIONAL, INC.,** a Delaware corporation, Defendant.	Case No.: 23-cv-02082 **JURY TRIAL DEMANDED**

COMPLAINT

Sheniqua Rowe ("Plaintiff"), through counsel, for her complaint against Defendant, Papa John's International, Inc. ("Defendant"), states:

NATURE OF THE CASE

1. This is an action to recover statutory damages arising out of Defendant's unlawful collection, receipt, use, and possession of the personal biometric identifiers and biometric information of Plaintiff in violation of the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 (2008).

THE PARTIES

2. Plaintiff is a natural person who is domiciled in Illinois and maintains her permanent residence in Chicago, Illinois.

3. Defendant is a corporation organized and existing in the state of Delaware.

4. Defendant maintains its principal place of business and nerve center at 2002 Papa John's Boulevard, Louisville, Kentucky.

5. Defendant operates and franchises pizza delivery and carryout restaurants and dine-in restaurants under the name "Papa John's." It operates over 5,500 locations - at least 500 company-owned restaurants and through more than 5,000 franchised restaurants in all fifty states in the U.S and in at least 48 countries and territories.

6. In Illinois, Defendant operates multiple restaurants as franchisor and/or owner.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(a) as the matter in controversy exceeds $75,000.00[1] exclusive of punitive damages, and/or interest and costs, and is between citizens of different States.

8. This Court has personal jurisdiction over Defendant because it conducts substantial business in Illinois.

9. Venue lies in this District pursuant to 28 U.S.C. §1391(b) as a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District.

RELEVANT FACTS

10. Non-party Ozark Pizza Company ("Ozark") is a franchisee of Defendant. It owns and operates 45 restaurants in Oklahoma, Arkansas, Missouri and Illinois.

11. Plaintiff was employed by Ozark to work at its Westchester restaurant location but also worked at one or more one of the restaurants that Ozark owns and operates at other locations in Illinois.

12. Plaintiff was a "shift leader" for Ozark and regularly had to work at multiple restaurant stores owned by Ozark and franchised by Defendant.

[1] Plaintiff seeks statutory, liquidated damages of $1,000 to $5,000 for each violation of BIPA and alleges that there were not less than 10,000 BIPA violations.

13. Plaintiff was employed by Ozark from 2014 through 2017[2].

14. Pursuant to Ozark's franchisee agreement with Defendant, Ozark uses a proprietary point-of-sale system, known as FOCUS, at its franchised restaurants.

15. Defendant developed and uses FOCUS in its company owned stores and in stores it franchises, including the store owned and operated by Ozark where Plaintiff was employed.

16. The FOCUS system includes a built-in fingerprint scanner.

17. Defendant requires its franchisees, including Ozark, to use FOCUS's fingerprint scanner "whenever possible" for employees to clock in and out, authenticate themselves to access the system, and input delivery routing.

18. During the period that Plaintiff worked for Ozark, she was required to use the FOCUS fingerprint scanner to: (1) clock in and out; (2) unlock FOCUS to input transactions; and (3) access other parts of the FOCUS system.

19. When an Ozark employee scanned his or her fingerprint into FOCUS for one of these reasons, the system compared the fingerprint to a reference fingerprint template of that employee stored in the system by Defendant.

[2] Plaintiff acknowledges that the applicable statute of limitations is five years as codified in 735 Ill. Comp. Stat. 5/13-205. *Tims v. Black Horse Carriers, Inc.*, 2023 IL 127801 (2023). This limitation period was tolled by the filing of the class action captioned *Kyles v. Hoosier Papa LLC and Papa John's International, Inc*. Case No. 1:20-cv-07146, pending in the United States District Court for the Northern District of Illinois, Eastern Division. The putative class in that action would include Plaintiff and is defined o as to include: "[a]ll individuals who used a fingerprint scanner connected to a FOCUS system in the State of Illinois at any point from December 3, 2016 to the present." See, *American Pipe & Construction Co. v. Utah*, 414 U.S. 538, 94 S.Ct. 756, 38 L.Ed.2d 713 (1974); *Crown, Cork & Seal Co. v. Parker*, 462 U.S. 345, 350, 103 S.Ct. 2392, 2395-96, 76 L.Ed.2d 628, 633 (1983).

20. Through FOCUS system's internet connection, Defendant has remote access to FOCUS systems at franchise locations through which it can download, collect data, and monitor fingerprint-scanner usage.

21. Ozark required its workers, including Plaintiff, to clock in and out of shifts and breaks with FOCUS's fingerprint scanner.

22. Ozark also required workers to use their fingerprints to unlock FOCUS for transactions.

23. As a shift leader, Plaintiff also scanned her fingerprints to log-in and log-out other Ozark employees and to perform the tasks associated with her position.

24. FOCUS has nine levels of user security clearance. Defendant used FOCUS's fingerprint scanner to control franchisees' and workers' access to various parts of the FOCUS system.

25. In addition to collecting fingerprints, Defendant using FOCUS collected and maintained reference templates derived from workers' fingerprints including those of Plaintiff.

26. Defendant using FOCUS then compared the reference templates against each subsequent fingerprint scan to identify the worker scanning in and associate the appropriate timekeeping and transaction information.

27. Defendant used the FOCUS system to remotely access Ozark's point-of-sale systems.

28. Defendant uses the FOCUS system's remote access to download and collect information from franchisees' point-of-sale systems, including Ozark's, daily. The point-of-sale system used by Plaintiff while employed by Ozark captured Plaintiff's biometrics and transmitted that information to Defendant.

29. Defendant used the FOCUS system's remote access to monitor fingerprint-scanner usage, including how the system was accessed and used by Plaintiff.

30. Defendant circulates reports identifying franchisees and workers who do not use the FOCUS system's fingerprint scanner, and instead use passwords for authentication.

31. Through its use of the FOCUS system, Defendant transmitted, disclosed and otherwise disseminated data including Plaintiff's biometrics to Ozark.

32. Through FOCUS, Defendant regularly downloaded data, including Plaintiff's biometrics, from that system and used that information in its business.

33. Through its use of the FOCUS system, Defendant exercised control over Plaintiff's biometrics and possessed that information.

34. Neither Ozark nor Defendant sought Plaintiff's consent prior to collecting fingerprint templates or fingerprint data through the FOCUS system.

35. Neither Ozark nor Defendant told Plaintiff how each would use the fingerprint data, how long each would store the data, or provide a publicly available retention policy regarding retention and storage of biometric data.

36. Defendant was required to destroy Plaintiff's biometric identifiers and information no later than three years after the conclusion of her employment and did not do so. Indeed, Defendant did not even have in place a post-employment retention and destruction policy at any time during Plaintiff's employment.

37. Prior to collecting and/or receiving Plaintiff's biometric identifiers and information, Papa John's International did not inform Plaintiff and the Papa John's International Class in writing that their biometrics were being collected, stored, and used.

38. Plaintiff did not consent to Defendant's disclosing any fingerprint data collected through FOCUS.

39. Plaintiff's fingerprints were scanned not less than 10,000 times during the course of her employment and during the applicable limitations period. [3]

HARM TO PLAINTIFF

40. While there are tremendous benefits to using biometric time clocks in the workplace, there are also serious risks. Unlike key fobs or identification cards—which can be changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with the employee. This exposes employees to serious and irreversible privacy risks. For example, if a fingerprint database is hacked, breached, or otherwise exposed, employees have no means by which to prevent identity theft and unauthorized tracking. If a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches or misuses – employees have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

41. A nefarious market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion

[3] *See*, fn. 2.

Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018).[4]

42. In late 2007, a biometrics company called Pay by Touch - which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions - filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records - which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data - could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used that company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

43. Recognizing the need to protect its citizens from situations like these, in 2008, Illinois enacted BIPA in light of the "very serious need [for] protections for the citizens of Illinois when it comes to [their] biometric information."[5]

44. BIPA was enacted with the understanding that "the full ramifications of biometric technology are not fully known." 740 ILCS 14/5(f). The legislature specifically found that persons who have their biometrics taken unlawfully are at increased risk of future injury. *Id.*

[4] Available at https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138.

[5] 95th Ill. Gen. Assem. House Proceedings, May 30, 2008, at 249 (statement of Representative Ryg), available at http://www.ilga.gov/house/transcripts/htrans95/09500276.pdf.

45. Biometrics are unlike other unique identifiers used to access finances or other sensitive information. "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[6]

46. To address this legitimate concern, Section 15(b) of BIPA provides that:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.[7]

47. For BIPA purposes, a "biometric identifier" is a personal feature that is unique to an individual and specifically includes fingerprints.

48. BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based upon an individual's biometric identifier used to identify the individual."[8]

[6] 740 ILCS 14/5(c).
[7] 740 ILCS 14/15(b).
[8] *Id.*

49. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it *first*:

> (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information."

740 ILCS 14/15(b).

50. BIPA specifically applies to employees who work in the State of Illinois.

51. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS 14/10.

52. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and—most importantly here—fingerprints. *See* 740 ILCS 14/10. Biometric information is separately defined to include any information based on an identifier that is used to identify an individual. *See id.*

53. BIPA also establishes standards for how employers must handle Illinois employees' biometric identifiers and biometric information. *See* 740 ILCS 14/15(c)-(d). BIPA makes it unlawful for companies to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." Furthermore, no company may "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless":

(1) the person or customer consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the person or customer;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

See 740 ILCS 14/15(c)-(d).

54. Ultimately, the BIPA is an informed consent statute. Its narrowly tailored provisions place no absolute bar on the collection, sending, transmitting or communicating of biometric data. For example, the BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does the BIPA limit to whom biometric data may be collected, sent, transmitted, or stored. The BIPA mandates that entities wishing to engage in that conduct must make proper disclosures and implement certain reasonable safeguards.

55. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's repeated violations of the BIPA alleged herein.

56. Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems that it used would be subject to the provisions of BIPA, a law in effect since 2008, yet wholly failed to comply with the statute.

57. Alternatively, Defendant negligently failed to comply with BIPA.

58. Plaintiff now seeks statutory, liquidated damages under BIPA as compensation for the Defendant's multiple violations of BIPA.

59. This lawsuit constitutes Plaintiffs' one and only chance at compensation for Defendant's violations of the BIPA. Depending on how technology evolves years into the future, losing control of and ownership over very personal identifiers could have untold harmful

consequences. The Illinois legislature concluded that the increased risk of future harm is a compensable loss under the BIPA, which is its right. *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 35, 129 N.E.3d 1197, 1206 citing 740 ILCS 14/5(c) (noting increased risk of identity theft should biometrics be compromised); *Dillon v. Evanston Hosp.*, 199 Ill. 2d 483, 507, 771 N.E.2d 357, 372 (2002) (Illinois Supreme Court finding risk of future injury compensable as an element of damages in medical malpractice case). The legislature's decision is particularly reasonable given that the statute of limitations on BIPA claims presumably runs from the date of the collection of biometrics, whereas the future injury may not occur until after the statute has run.

60. Given that this harm is difficult to quantify, assignment of liquidated damages is appropriate.

COUNT ONE

Violation of §15(a) of BIPA
[Failure to Institute, Maintain, and Adhere to Publicly Available Retention Schedule]

61. Plaintiff restates paragraphs 1 through 60 of the complaint as if set out here in full.

62. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention - and, importantly, deletion - policy. Specifically, these companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 15(a).

63. Defendant is an entity registered to do business in Illinois and thus it qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

64. Plaintiff is an individual who had "biometric identifiers" (in the form of fingerprints) collected by Defendant. *See* 740 ILCS 14/10.

65. The Plaintiff's biometric identifiers were used to identify her and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

66. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 15(a).

67. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's biometric data and has not destroyed Plaintiff's biometric data when the purpose for collecting or obtaining such data has been satisfied or within 3 years of the individual's last interaction with the company.

68. By collecting, storing, and using Plaintiff's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's privacy in her biometric identifiers or biometric information as set forth in BIPA *each time* the Defendant collected, stored or used Plaintiff's or the Class's biometric identifier. *See* 740 ILCS 14/1, *et seq*.

69. Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with the statute.

70. Alternatively, Defendant negligently failed to comply with BIPA.

71. Plaintiff seeks statutory, liquidated damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory, liquidated damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT TWO

Violation of §15(b) of BIPA
[Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information]

72. Plaintiff restates paragraphs 1 through 60 of the complaint as if set out here in full.

73. BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b) (emphasis added).

74. By collecting Plaintiff's fingerprints through FOCUS, Defendant collected Plaintiff's biometric identifiers. 740 ILCS 14/10.

75. By capturing and maintaining reference templates and associated timekeeping and transaction information, Defendant collected Plaintiff's biometric information. 740 ILCS 14/10.

76. Prior to collecting Plaintiff's biometric identifiers and information, Defendant did not inform Plaintiff in writing that her biometrics were being collected, stored, and used. 740 ILCS 14/15(b)(1).

77. Prior to collecting Plaintiff's biometric identifiers and information, Defendant did not inform Plaintiff of the specific purpose for which her biometrics were being collected, stored, and used. 740 ILCS 14/15(b)(2).

78. Prior to collecting Plaintiff's biometric identifiers and information, Defendant did not inform Plaintiff of the length of time that her biometrics would be maintained. 740 ILCS 14/15(b)(2).

79. Prior to collecting Plaintiff's biometric identifiers and information, Defendant did not obtain a written release authorizing such collection. 740 ILCS 14/15(b)(3).

80. Defendant is an entity registered to do business in Illinois and thus it qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

81. Plaintiff is an individual who had "biometric identifiers" (in the form of fingerprints) collected by Defendant. *See* 740 ILCS 14/10.

82. The Plaintiff's biometric identifiers were used to identify her and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

83. By collecting, storing, and using Plaintiff's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's privacy in her biometric identifiers or biometric information as set forth in BIPA *each time* the Defendant collected, stored or used Plaintiff's or the Class's biometric identifier. *See* 740 ILCS 14/1, *et seq*.

84. Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with the statute.

85. Alternatively, Defendant negligently failed to comply with BIPA.

86. Plaintiff seeks statutory, liquidated damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory, liquidated damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

and reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT THREE

Violation of §15(d) of BIPA
[Disclosure of Biometric Identifiers and Information Without Obtaining Consent]

87. Plaintiff restates paragraphs 1 through 60 of the complaint as if set out here in full.

88. BIPA prohibits private entities from disclosing or otherwise disseminating a person's or customer's biometric identifier or biometric information without obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

89. By using and sharing FOCUS's biometric, timekeeping, and transaction data with Ozark, Defendant disclosed or otherwise disseminated Plaintiff's biometric identifiers and information.

90. Defendant is an entity registered to do business in Illinois and thus it qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

91. Plaintiff is an individual who had her "biometric identifiers" (in the form of her fingerprints) collected by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

92. Plaintiff's biometric identifiers were used to identify her and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

93. By disclosing, redisclosing, or otherwise disseminating Plaintiff's biometric identifiers and biometric information without her consent as described herein, Defendant violated BIPA *each time* there was a disclosure, redisclosure or dissemination of the Plaintiff's biometric identifiers in violation of Plaintiff's right to privacy in her biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

94. Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with the statute.

95. Alternatively, Defendant negligently failed to comply with BIPA.

96. Plaintiff seeks statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, respectfully request that the Court enter judgment in her favor and against Defendant for statutory, liquidated damages for each of Defendant's violations of the BIPA, pursuant to 740 ILCS 14/20; and award Plaintiff reasonable litigation expenses and attorneys' fees.

JURY DEMAND

Plaintiff hereby respectfully demands a trial by jury.

Respectfully submitted,

SHENIQUA ROWE

/s/ Nick Wooten
DC Law, PLLC
1012 West Anderson Lane
Austin, Texas 78757
(512) 220-1800
nick@texasjustice.com

Rusty A. Payton
DC Law, PLLC
20 North Clark Street
Suite 3300
Chicago, Illinois 60602
(773) 682-5210
rusty@chicagojustice.law

Counsel for Plaintiff